Integrity projects

Ministry of the Interior
National Security Service (BVD)

PER·UNDAS · ADVERSAS

L.S.,

One of the tasks set for the Dutch security service (BVD) is to promote adequate security for major national interests. The integrity of the system of democratic legal order in the Netherlands is considered to be one of these interests.
BVD develloped a method enabling civil services to make an inventory of their vulnerabilities for attacks on their integrity, both from the inside and from the outside of the organisation.
This brochure gives a brief outline on the underlaying filosophy and on the structure of the method.

Contents

1 The importance of integrity

"The government is either incorruptible or it is corruptible. There is nothing in-between. Integrity is unconditional. And integrity is vital to the functioning of administration; violation of integrity in the public sector means nothing less than that the government loses the confidence of the citizens. And democracy cannot do without the confidence of the citizens. It would mean the end of democracy. That is a depressing idea."

With these crystal-clear words Mrs Dales, Minister of the Interior, concluded her speech at the annual congress of the Association of Netherlands Municipalities at Apeldoorn in 1992. Her words sparked a debate, not only within the Association, but also in other sections of the public sector, the end of which is still not in sight.

Misuse of power within the public sector, decay, decline and loss of (democratic) values and standards are phenomena to be taken seriously. Particularly because these phenomena may easily lead to fraud and corruption. In the event of a cumulation of integrity violations in the public sector the reputation of the government would be in jeopardy. It makes little difference whether such violations take place in only one section of a government organisation. A breach of integrity within one section always has its repercussions on other sections and may soon affect the functioning of the whole organisation.

If, moreover, the number of thus disreputed government bodies is increasing, (confidence in) our democratic legal order may be undermined in the long term. That accounts for the involvement of an organisation such as the National Security Service (BVD) in finding solutions to these problems.

2 The importance of a preventive integrity policy

A reputation of integrity is not self-evident, but it is a merit that should be deserved every day. The consolidation of such a reputation demands continuous attention. The first and principal responsibility rests with the parties most concerned: public administration and the management of the government agency concerned. After all, violation of integrity can be regarded as an undermining of the proper functioning of an organisation. The management can be held responsible for that functioning. In other words, integrity is a management issue.

Moreover, the management of a government organisation is in a position to tackle integrity-related problems, even if the objectionable practices are not instigated by employees of the organisation concerned but by outsiders. However, government bodies should be wise enough not to ascribe violations of integrity to malicious outsiders alone. Whatever objectionable practices outsiders have in mind, the decisive factor is how insiders in the government body handle it. In other words: the turning point between integrity and corruptibility always is within the government organisation itself. Consequently each government body has the possibility to tackle fraud and corruption, to fight and especially prevent these and other forms of integrity violations.

Integrity is not an alien or remote phenomenon in the public service. Integrity should be given as much attention in the daily routine as micro-economic elements such as effectiveness and efficiency or input and output. However, an integrity policy can only be placed on a solid footing when the management recognizes the potential risks in the organisation and is prepared to make investments in integrity. A logical first step towards an effective integrity policy is to investigate the organisation by making an assessment of the potential risks. After all, for making specific investments one needs to know where such investments are necessary, in other words, where integrity is threatened.

The activities of the BVD in this field are part of the preventive policy project of the Ministry of the Interior. This project provides for a prevention programme consisting of the following seven steps:

1. Investigation of the organisation, including
   a establishing what specific sections and departments of the organisation should be considered vulnerable. For the realization of this step the BVD has developed a method to expose the intrinsic vulnerability of certain sectors in the organisation. In chapter 5 this method will be explained in detail.

   b making an inventory of vulnerable positions. If the vulnerability of these positions is such that it might damage the national security or other important interests of the state, the positions are designated as 'positions involving confidentiality'. Applicants for a position involving confidentiality have to undergo security screening carried out by the BVD.

3 Threat

Integrity is a precondition for the proper functioning of the public sector. However, this functioning has become increasingly complicated in the last few years. This can be ascribed to a number of developments:

- the increasing complexity of society (less recognizable social arrangements and differentiation of values and standards);
- the entwinement of public and private interests as a result of government involvement in networks and public/private partnerships;
- aggressive lobbying by economic and social organisations in order to promote mostly conflicting interests;
- the fact that it has become increasingly difficult for the government to solve a widening range of complicated economic and social problems by means of adequate rules and regulations;
- the (economic and financial) need to tackle these problems with reduced manpower and resources (micro-economic management)
- the development of a policy of toleration as an administrative instrument;
- the increasing globalization as a result of the participation of national governments in international structures (especially related to the unification of Europe).

This enumeration is not exhaustive. And each individual development or a combination of some of them do not inevitably lead to breaches of integrity in the public sector. However, it seems that gradually a climate is developing in which inhibitions and barriers against corruption are eroding.

There is something else. We should bear in mind that certain people want to take advantage of the situation. In this connection we tend to point our finger at the growing impact of organised crime, both inspired in the Netherlands and in other countries. It is a fact that criminal organisations seek to consolidate or, if possible, expand their illegal activities. To that end they do not always adopt a passive attitude towards their natural opponent, the government.

However, violations may also be inspired by basically lawful organisations and individuals. Especially when economy is faced with setbacks, major interests are at stake in the relations between companies and social organisations on the one hand and the government on the other. The temptation to misappropriate goods or services that cannot be obtained lawfully is not a negligible factor. In addition, the conflict of interests between government and cost-conscious citizens should not be lost sight of. Finally, integrity may also be undermined by a civil servant while no outsider is involved, for instance when it concerns matters such as theft or when a person uses official knowledge or powers to his own advantage.

2. Protection of the integrity of the organisation;
3. Systematic control of the engagement of new personnel;
4. Drawing up a code of conduct for the employees;
5. Keeping the code of conduct alive;
6. Supervision of the compliance with the code of conduct;
7. Developing measures to be taken in the event of (a risk of) intolerable activities.

The Minister of the Interior informs the parliament through regular progress reports about the implementation and state of affairs of the (preventive) integrity policy. The activities of the BVD are incorporated in these public progress reports.

In principle violations of integrity can be divided into two types.
The first variant implies that an employee gains improper personal benefit at the expense of the organisation he is employed with (theft, abuse of knowledge or powers, fraud).
The second variant implies that an employee benefits an outsider at the expense of the organisation. This may take place both on a voluntary basis (due to corruption or conflicting interests and loyalties) and on an involuntary basis (under pressure of blackmail or force exerted by an outsider).
The improper benefit gained by an outsider may concern:

- material advantages, such as money (subsidies, orders, tenders), goods (passports, driving licences) and services (licences);
- immaterial advantages, such as illicitly obtained information (in the form of confidential data which enables the outsider to consolidate or expand his position).

Also when an outsider seeks to profit from a government organisation, the weak spot is always within the organisation itself, as described under the first variant. Obviously in both situations the crucial question is whether and to what extent public servants are prepared to gain or provide improper benefit, which leads to a violation of integrity.

4 Defence

Speaking about the ability of an organisation to defend itself against violations of integrity (intrinsic resistance), one should realize that corruptible behaviour is virtually always secretive behaviour. That makes it difficult to recognize and even more difficult to prove such behaviour.

Besides, government bodies usually pretend to be incorruptible. Any suspicions to the contrary are outweighed by these pretensions. Consequently, persons who spot behaviour which might indicate a breach of integrity do not always find a ready ear within the hierarchic structure of the organisation concerned.

The higher echelons are often inclined to claim that 'in this organisation everything is okay'. More than once it is the fate of the civil servant who raises the alarm to be treated as the proverbial messenger bringing bad news. And those who are actually involved in intolerable activities usually appeal to the 'natural' pretensions of integrity to keep out of reach, or sometimes even to eliminate the person who raised the alarm.

But also government bodies that do not consider their integrity to be beyond all doubt do not always take adequate steps when they perceive a breach of integrity in their organisation. They wrongly presume that taking such steps will cause unrest and will add to the damage to the organisation. In practice this attitude is particularly adopted when a senior official is suspected. In such cases it is usually considered preferable to hush up rather than expose the objectionable activities. This does not help to improve the ability of the organisation to defend itself against violations of integrity, because the organisation is not cleared of the suspicions. Moreover, when the hush up turns out to be not very effective and the media or other outsiders expose the covered up abuses, the breach of integrity often proves to be considerably more substantial than when adequate measures are taken at an early stage.

It is evident that the aforementioned differentiation of values and standards in society also pressurize the moral standards within the public sector. The social position of the civil servant and what he should do or not do, have become less clear and obvious. The civil servant is more and more confronted with the dilemma: do I have to refrain from doing what is not formally permitted or am I allowed to do what is not formally prohibited. This latitude may encourage violations of integrity.

On the basis of the above-described circumstances the risk of a breach of integrity in the public sector should be taken seriously. For that reason it is of the utmost importance that every government body is aware of - and has a realistic idea of - its own potential vulnerability. Awareness is the first condition to give shape to the protection of integrity. The second step in this process is to improve the ability of the organisation to defend itself against violations of integrity (boost the resistance).
Through both regular and specific provisions and measures each organisation in the public sector can largely prevent violations of integrity and anyway fight them.

5 Guidelines for investigations into integrity-related vulnerability

In the booklet called 'Integrity is unconditional' the BVD has laid down guidelines intended to enable organisations in the public sector to set up an integrity project covering the following steps:

stage A the identification of vulnerable activities carried out in various sections of the organisation (in order to get an idea of the potential integrity-related risk posed to that organisation);

stage B assessment of the existing defence against violations of integrity (in order to define whether and to what extent the potential risk is an actual risk);

stage C the formulation of additional provisions and measures in order to increase the ability of an organisation to defend itself against violations of integrity, if necessary (in order to restrict the actual risk to a minimum).

The methods described in the guidelines are largely based on what the BVD learnt from integrity surveys it has carried out in various organisations in the public sector since 1993 and on earlier publications of the Ministry of the Interior about measures, instruments and methods for the protection of integrity .

During stage A of the project an inventory is made of the vulnerable activities carried out in the organisation. It concerns activities which, if not carried out properly, might entail improper benefit for members of staff or outsiders. It is necessary to know what these activities include and in which sections of the organisation they are carried out in order to assess where a breach of integrity might be expected. An overview of vulnerable activities has been given in table 1 (activities related to the handling of information, money, goods and services within a government body) and table 2 (activities related to the external tasks of a government body).
In order to identify and trace vulnerable activities it is advisable first to consult the senior management (through interviews). The management should also answer the question what type of vulnerable activities might entail the greatest risks to the organisation. The findings of this stage of the investigation should be laid down in a report that can be distributed in the organisation after the management has given its consent.

Stage B is intended to make an assessment of the existing defence against violations of integrity. The ability of an organisation to prevent such violations is dependent on a number of elements in the structure and culture of the organisation.
In the guidelines it is advised to investigate these elements along three lines.

The first line focuses on the existing regulations pertaining to activities which were denoted as vulnerable during stage A of the investigation. The relevance of these regulations to the defence of an organisation against violations of integrity appears from the following three aspects:

- the organisation provides clarity to its staff about the proper way to carry out vulnerable activities;
- the organisation promotes uniform operating procedures which makes it more difficult to act at one's own discretion (arbitrariness);
- through control elements the organisation can check whether the activities are indeed carried out carefully and properly.

The second line concerns mainly the selection of personnel and job descriptions. First of all the recruitment and appointment policy of the organisation should be checked. In order to find out whether sufficient information on applicants is collected to have a reasonable indication that their functioning will be honourable and incorruptible, some interviews should be held with employees of the personnel department and recently appointed employees.

Subsequently, interviews with employees of the personnel department should show whether the job descriptions meet the requirements for consolidating integrity (the so-called integrity requirement). It is essential that the organisation provides clarity to each individual employee about his duties and (limits of) powers in order to prevent him from acting on his own authority. Vague job descriptions offer too much scope for personal initiatives, a latitude which might lead to a breach of integrity.

The third line examines a large number of interrelated elements involved in integrity awareness through a survey of the staff. The principal issues in the survey are:

- the alertness of the staff (awareness of vulnerable activities in one's own job);
- the clarity provided to employees on the proper execution of vulnerable activities (co-ordination of tasks and powers, availability of job descriptions, and the existence of, and familiarity and compliance with regulations for the performance of vulnerable duties);
- the supervision of the proper execution of vulnerable activities (control and accountability);
- the explicit attention for the integrity requirement within the organisation (integrity as an item to be discussed during discussions of progress and job appraisal interviews);
- the thresholds against entanglement of interests (regulations pertaining to business gifts, additional functions and additional income);
- tensions between private and office life (how to make private problems discussable, how to handle business matters touching private life);
- how to deal with incidents related to violations of integrity.

Finally the survey contains a number of statements on which the respondents should comment. This should provide an insight into four aspects relevant to the ability of the organisation to defend itself against breaches of integrity. These aspects are: legitimacy versus efficiency, loyalty, (internal) communication and self-correction.

The results of the three-line investigations during stage B show whether and in what form the organisation faces a risk of a violation of integrity. The stage A report serves as a frame of reference. Prior to making conclusions about the defence against violations of integrity, the findings of stage B are submitted to part of the respondents. Subsequently the findings and the feed-back discussions are incorporated in a report, which is to be distributed in the organisation after the management has given its consent.

On the basis of the reports of stages A and B the management can decide whether the defence of the organisation should be enhanced. In that case a set of measures and provisions can be formulated during stage C.
The guidelines give various suggestions for such measures, related to the elements investigated during stage B which determine the level of defence. These options have been listed in table 3. They are mostly based on the intrinsic abilities in every organisation to raise the level of defence against violations of integrity. In addition, a number of specific measures are suggested and explained. It concerns positions involving confidentiality, the formulation of a code of conduct, the appointment of counsellors and the realization of specific integrity-related projects intended to remain alert, the so-called alertness programmes.

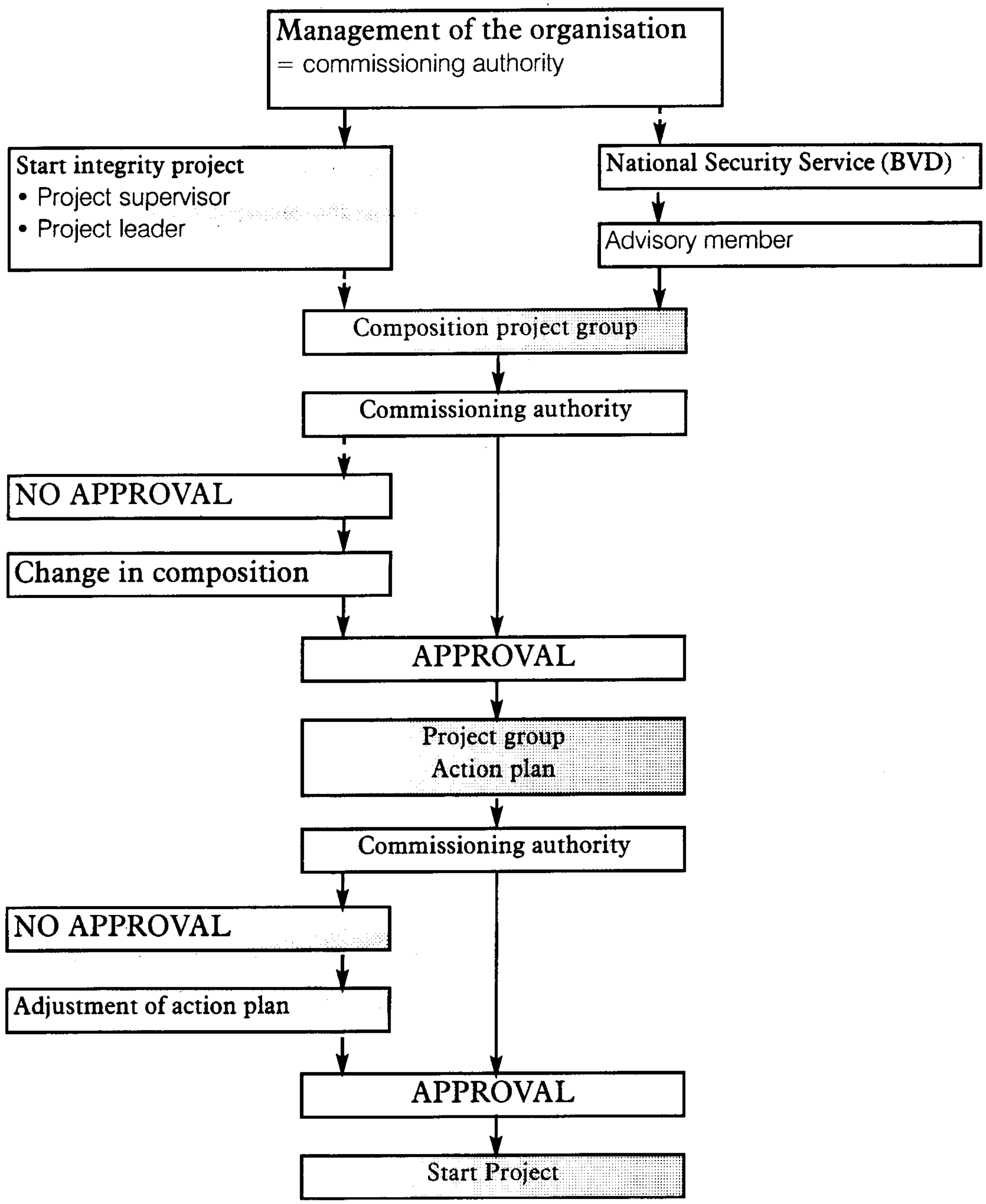
Obviously the list of options in table 3 is not exhaustive . It is quite possible that on the basis of the acquired knowledge about specific vulnerability and defence the organisation finds alternative means to reduce the risk of a breach of integrity.

The report of stage C provides an overview of the total set of measures and provisions to be introduced by the management in order to correct the inadequacies in the organisation's ability to defend itself against violations of integrity.
The approval of the report by the management and its distribution within the organisation mark the end of the integrity project.

Diagram 1

Preparatory phase of an integrity project

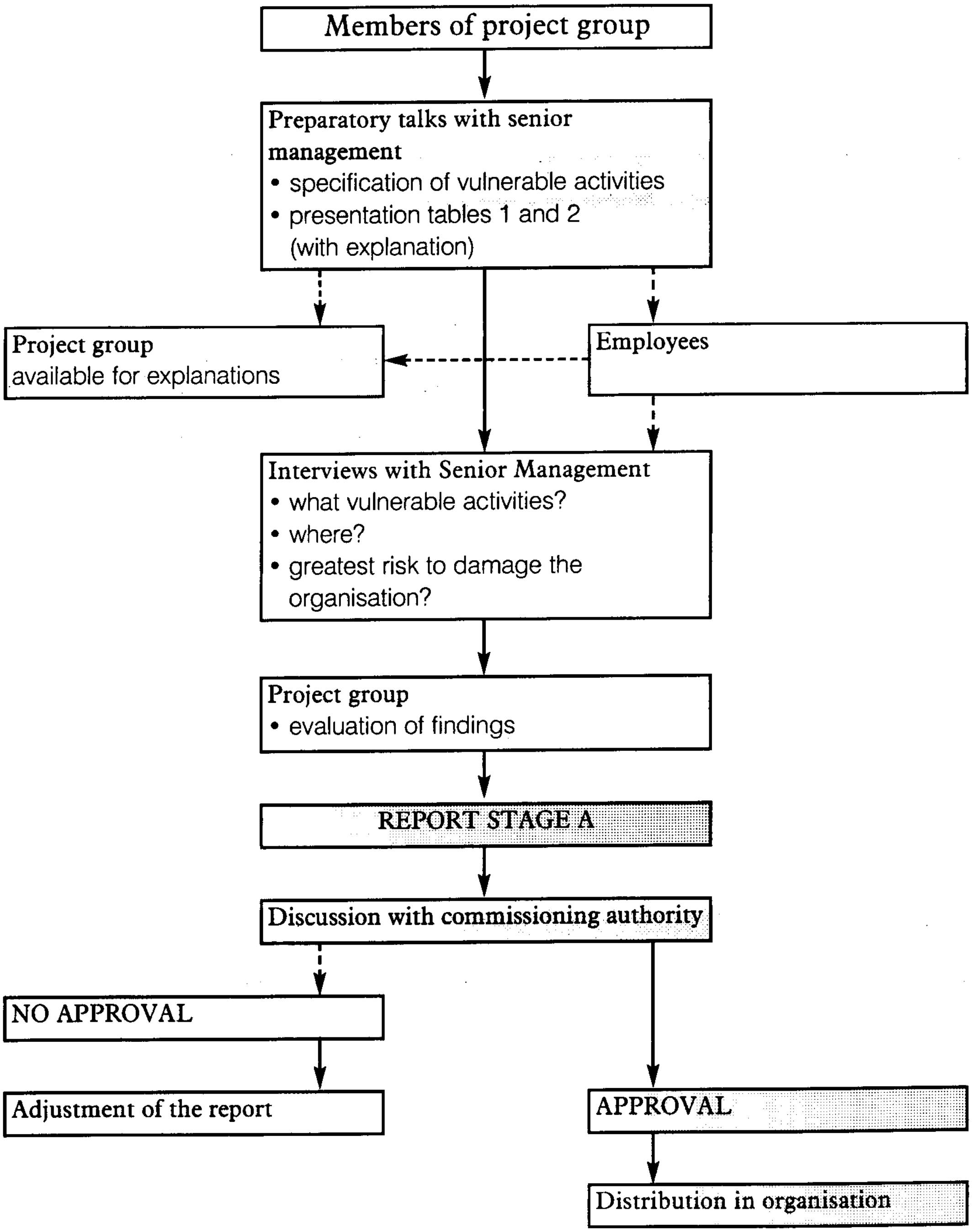
10



Start Stage A

Diagram 2

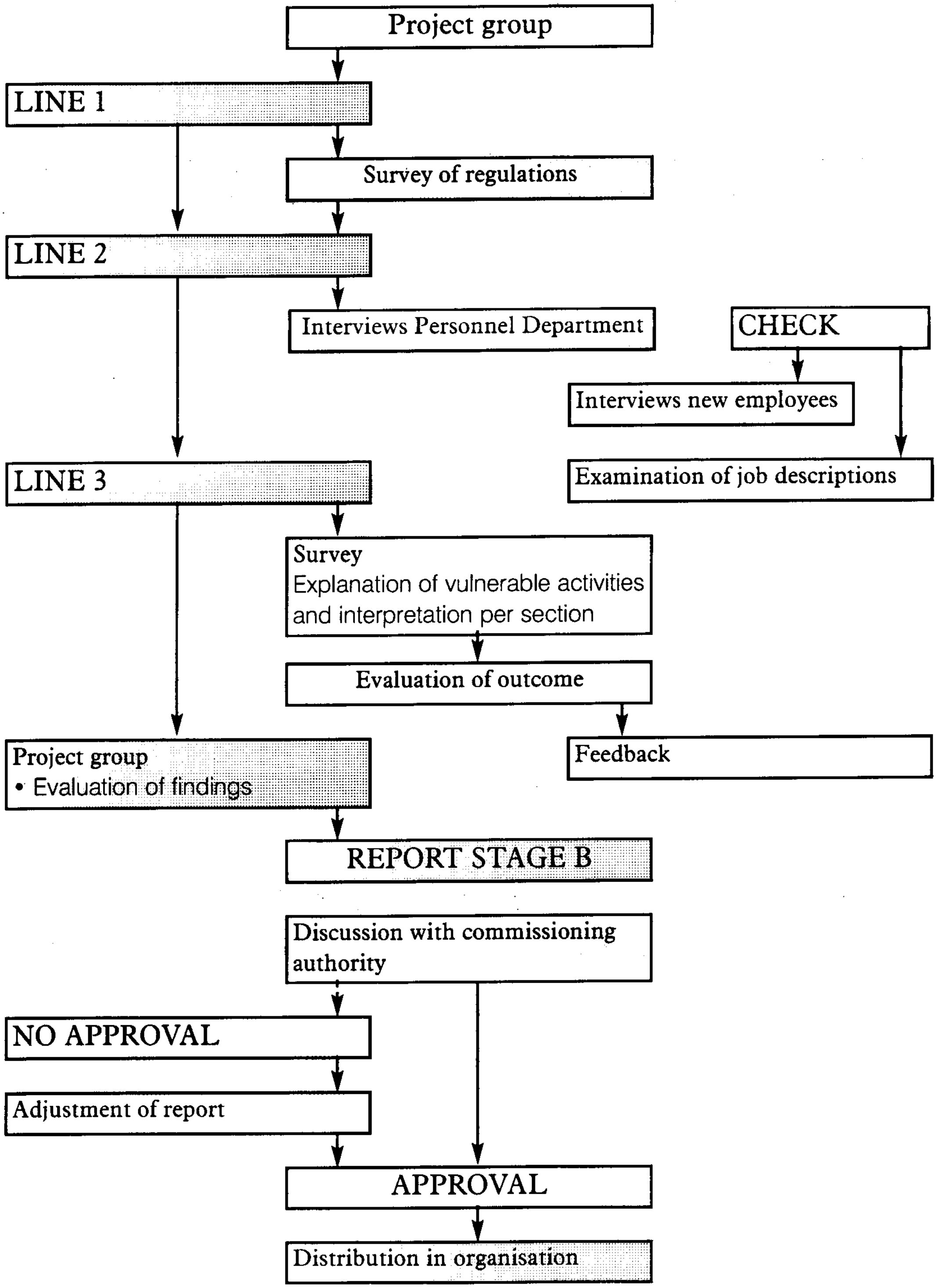
Stage A: The identification of vulnerable activities


Members of project group
Preparatory talks with senior management
• specification of vulnerable activities
• presentation tables 1 and 2 (with explanation)
Project group
available for explanations
Employees
Interviews with Senior Management
• what vulnerable activities?
• where?
• greatest risk to damage the organisation?
Project group
• evaluation of findings
REPORT STAGE A
Discussion with commissioning authority
NO APPROVAL
Adjustment of the report
APPROVAL
Distribution in organisation

Start Stage B

Diagram 3

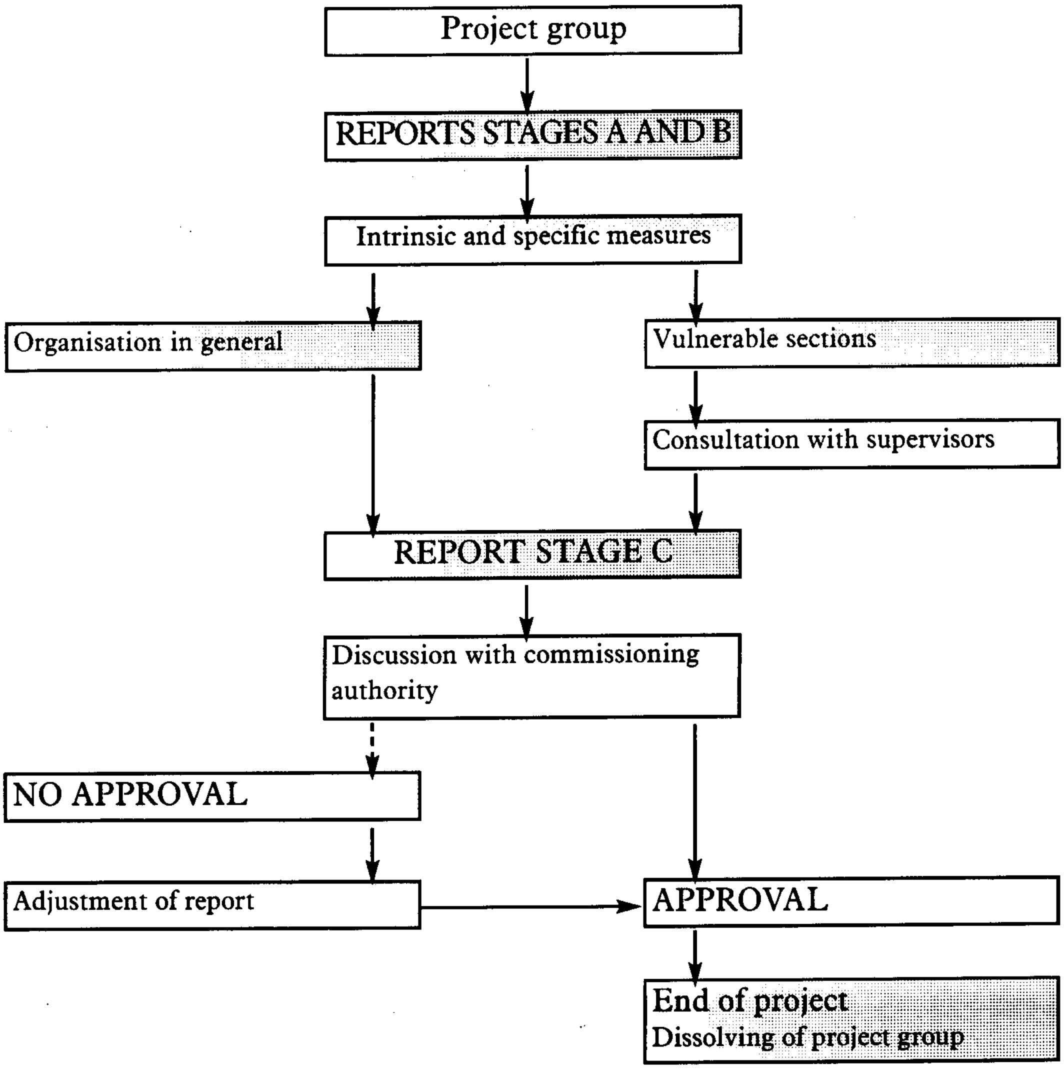
Stage B: Assessment of the existing defence



Start Stage C

Diagram 4

Stage C: increase of the defence



Implementation

Responsibility management of the organisation

6 Introduction of a project

A precondition for the success of an integrity project is the willingness of the management of a government body, but also of its staff, to seriously tackle the problem of integrity. After all, the described integrity project is a self-examination. It requires efforts and cooperation of the members of the organisation, while eventually they should also be prepared to take measures against inadequacies. If there is no willingness to do this, the project is doomed to fail from the outset.

Starting from this willingness, the unambiguous decision of the management of the government organisation concerned marks the beginning of an integrity project. As violations of integrity can be regarded as an undermining of the proper functioning of an organisation, such violations are primarily a concern of the management of that organisation. The management not only bears responsibility, but it is also in a position to give shape to the protection of integrity.

The BVD guidelines for an integrity project are based on the principle that the management of the organisation acts as commissioning authority. After the decision to start an integrity project, the management has to appoint a project leader who is entrusted with forming a project group. One of the members of this project group should be project supervisor. The supervisor acts as a contact person for the project group on behalf of the commissioning authority. He also has a mandate to provide the project group with resources during the various stages of the project. Prior to the actual start of the project the project group submits an action plan or project plan to the commissioning authority for approval.

In principle the BVD is prepared to consider whether it might play an assisting and advisory role in the project. If the authority that decides to commission a project shows a preference for BVD assistance, agreements should be made during the preparatory stage. Experience has shown that good cooperation can be realized by adding a BVD security adviser as an advisory member to the project group. His knowledge of integrity problems and his experience with integrity projects in other organisations may help the project group from the outset.

Diagram 1 shows the preparatory stage of the project. Diagram 2 gives an outline of stage A, the identification of vulnerable activities. Diagram 3 describes stage B, the assessment of the existing defence. Finally, diagram 4 sketches the final stage of the investigation, when recommendations are formulated for enhancing the organisation's ability to defend itself against breaches of integrity.

7 Start of an integrity project

In order to get the required support for both the start of an integrity project and the steps to be taken after its conclusion, it may be necessary to inform the political authority responsible at an early stage, especially when an organisation coming under public administration is concerned. In order to avoid surprises at a later stage, the management of the organisation is recommended to take such initiatives during the preparatory phase. In addition, as we stated before, the cooperation of the staff of the organisation (managers and employees) is indispensable for the realization of the project. It is advisable to inform the employees council (Works Council) about the project during the preparatory stage in order to prevent any misunderstanding about the management's intentions. It is also essential that the staff as a whole receives sufficient information about the following aspects before the actual commencement of the project (and if possible also before the start of a new stage):

- the importance of protection of integrity in the organisation;
- the decision of the management to start an integrity project;
- the aims and general contents of the project;
- the composition of the project group;
- the (possible) participation of a BVD officer as an advisory member;
- the fact that the project was not inspired by mistrust of personnel.

Particularly the last-mentioned aspect is of crucial importance. Experience has shown that when an integrity project is started, one can easily, unintentionally, create the impression that the management of the organisation has doubts about the attitude or behaviour of the employees. This impression should anyhow be avoided or removed, as the input of the employees is essential for the success of the project. It is especially day-to-day routine which enables the employees to clearly identify vulnerability and make valuable suggestions to improve integrity awareness.

The project supervisor and the project leader are the most appropriate persons to give the above-described information to the employees. There are various options to realize this. In a small organisation a plenary meeting of all personnel can be a good opportunity. Larger organisations have had good experiences with a circular letter to the personnel or with an interview of the supervisor and/or leader of the project in the personnel magazine.

8 Incidents

An integrity project is definitely not intended to test the personal integrity of the employees in an organisation. Nevertheless, it cannot be ruled out that during the progress of the project the project group is confronted with (suspicions of) actual violations of integrity.

It is of great importance that the progress of the project is not disturbed by such incidents. After all, the project was not set up to track down any abuses. The project group should refer employees who think to know something about a (possible) violation of integrity to the management of the organisation. The management is responsible for dealing quickly and adequately with incidents. That is the only way to show the employees that the management attaches great value to integrity in general and to the integrity project in particular. It is not the task of the project group to investigate reported incidents. That is not the responsibility of the project group and it might jeopardize the required cooperation of all employees.

Incidents may also be reported to the Registration Centre for integrity-related incidents which comes under the responsibility of the BVD. This Registration Centre has a supplementary function. That means that individual employees should preferably first discuss the (suspected) violations within their own organisation. The BVD's Registration Centre for violations of integrity only seeks to help persons who feel inhibitions to report a breach of integrity to their superiors or who are not in a position to do so.
The BVD sees to it that the person who reports remains anonymous in order to keep the threshold as low as possible. Each report is followed up, in order to find out whether and if so in what form a violation of integrity has taken place or threatens to take place. Such investigations are restricted to the verification of facts and circumstances, either by letter or by (further) interviews with the person who reports or with third parties. If it turns out that it really concerns a (potential) breach of integrity, the organisation involved is informed about it. When there is evidence to suggest that offences have been committed, the organisation is recommended to contact the Public Prosecutions Department.

Table 1

Vulnerable activities related to the handling of information, money, goods and services within a government organisation

Internal organisation	Vulnerable activities in general	Examples of specific activities
Information	Activities related to confidential information; both production and awareness and the handling of classified or other confidential documents, files and (computerized) data bases	• holding (inside) information • the provision of confidential information • the examination of confidential documents (files) • the production of confidential documents • the classification of confidential documents • the administration (storing) of confidential documents • the duplication of confidential documents • taking confidential documents outside the building • the input of confidential data into files • the mutation of confidential data in files • the administration of confidential files
Money	Activities related to cash or giro-based funds in the form of budgets, statements of expenses, bonuses, premiums, allowances, etc.	• the allocation of budgets • the control of budgets • auditing expense claims • granting expense allowances • payment of expenses • granting bonuses, premiums, allowances • payment of bonuses, premiums, allowances
Goods and Services	Activities related to both the purchase, administration and use of goods (inventory, computers, company cars, etc.) and hiring services (counselling, security, cleaning, catering, etc.)	• making decisions about purchase or hiring • setting quality requirements or terms of delivery • requesting quotations • carrying on negotiations • assigning suppliers • the administration of goods within the organisation • the allocation of goods within the organisation • using company goods outside office hours or outside the office

Table 2

Vulnerable activities related to the external tasks of a government organisation

External tasks	Vulnerable activities in general	Examples of specific activities
1 Collection	Activities related to tax assessments, premiums, excise, administrative charges, etc.	• the verification of tax returns • the application of assessment criteria • the determination of the amount due • the imposition of an obligation to pay • debt collection
2 Contracting out	Activities related to orders, invitations to tender, contracts, etc.	**concerning invitations to tender:** • budgetary control • making specifications, quality requirements • the selection of a form of tender (public or private) • assessment of tenders • negotiation • the selection of contractors • inspection of the execution • giving permission to extra work • inspection on delivery or completion
3 Payment	Activities related to subsidies, premiums, allowances, sponsoring, benefits, etc.	• the verification of applications • the application of assessment criteria • the determination of the amount to be paid • deciding to pay • payment of the awarded amount
4 Granting	Activities related to licences, driving licences, passports, identity cards, authorizations, etc.	**concerning licences:** • (if applicable) the imposition of licencing obligations • the verification of applications • the application of assessment criteria • (if applicable) the formulation of terms and conditions • checking the compliance

External tasks	Vulnerable activities in general	Examples of specific activities
5 Enforcement	Activities related to supervision, control, investigation, prosecution, execution, etc. (related to compliance with or violation of the law)	• setting priorities in supervision or control • the selection of targets or target groups in supervision or control • the establishment, registration or reporting of offences • the detection of offences • arresting suspects, perpetrators, offenders • instituting proceedings against suspects • imposing punishments, sanctions, fines • the execution of punishments or recovering fines • granting temporary release or giving a pardon, the remission of fines

Table 3

Defence

Aspects	Problems	Suggestions for possible solutions
1a Regulations pertaining to vulnerable activities: PRESENCE	No (or incomplete) regulations; risk: • no uniform procedures • insufficient thresholds against abuses • acting at one's own discretion	Draw up regulations for all (categories of) vulnerable activities
1b Regulations pertaining to vulnerable activities: CONTENT	Regulations are insufficiently focused on integrity requirement; risk: • insufficient provisions to prevent solo actions • insufficient control elements, provisions for supervision	Discourage solo actions and improve supervision through the formulation of regulations pertaining to: • teamwork • separation of duties • joint decision-making • accountability (structural reporting) • structural supervision • unambiguous criteria for evaluation • written accounts of activities and decisions
1c Regulations pertaining to vulnerable activities: FAMILIARITIY	Insufficient familiarity with the regulations; risk: • no uniform procedures • acting at one's own discretion	Improve familiarity with the regulations by: • wide distribution • general accessibility
1d Regulations pertaining to vulnerable activities: APPLICATION	Inadequate application of the regulations; risk: • arbitrariness	Encourage application of the regulations by: • exemplary conduct (of the management) • supervision • imposing sanctions in the event of non (or mis) application
2 Selection of personnel	Insufficient attention for integrity requirement; risk: • insufficient insight into integrity of (future) personnel • insufficient attention for vulnerable aspects of the new job (leading to reduced alertness, awareness)	Selection and appointment via: • consistent application procedures • requiring extensive CVs • requiring and verification of references • enquiries about performance in previous jobs • verification of original diplomas and certificates • requiring a certificate of good behaviour • informing applicants about integrity aspects involved in the position • taking the oath (or solemn affirmation) of office (integrity requirement) • introduction programme (attention for integrity)

Aspects	Problems	Suggestions for possible solutions
3 Training and information material	Omission of an important means to draw attention to the integrity requirement; risk: • reduced alertness • reduced awareness	Enhance integrity-related alertness and awareness by drawing specific attention to the integrity requirement in • courses • information material
4 Job descriptions	No or not updated, incomplete or imprecise job descriptions; risk: • insufficient clarity about duties and powers • acting at one's own discretion	Provide clarity on duties and powers through up-to-date, complete and precise job descriptions
5a Vulnerable activities AWARENESS	No awareness; risk: • insufficient alertness to vulnerable aspects of the job	Improve awareness through: • adequate job descriptions (cf. 4) • information (cf. 3) • consultations (cf. 7)
5b Vulnerable activities PROVISIONS	No or inadequate provisions /measures; risk: • acting at one's own discretion • development of ad-hoc structures • great pressure on personal interpretation of integrity • insufficient caution in the performance of duties	Make sure that vulnerable activities are carried out properly through: • extra guidance • teamwork • adequate replacement in case of absenteeism • periodic job rotation • control (cf. 9) • consultations (cf. 7) • designating vulnerable positions as positions involving confidentiality • imposing sanctions on improper performance
5c Vulnerable activities CUMULATION (cf. stage A)	Many (types of) vulnerable activities combined in one position; risk: • inadequate concentration	Make the risk controllable through: • separation of duties
6a 'Grey area' PRESENCE	Virtual powers have wider scope than formally permitted; risk: • lack of clarity about lawfulness of activities and decisions	Remove 'grey area' through: • adequate job descriptions (cf. 4)
6b 'Grey area' CONSULTATION AND ACCOUNTING	No prior consultation, nor evaluation afterwards; risk: • lawfulness not checked • mistakes not detected or corrected Only evaluation afterwards; risk: • correction only possible when mistakes have already been made Occasional prior consultation or evaluation afterwards; risk: • arbitrariness	Guarantee lawfulness of activities in 'grey area' through consistent prior consultations (optimum threshold) or evaluation afterwards (minimal threshold)

Aspects	Problems	Suggestions for possible solutions
7a On-the-job consultation AVAILABILITY OF SUPERVISOR	Supervisor not available for quick consultation; risk: • solo action • acting at one's own discretion	Prevent solo action and improve control by: • adequate availability of the supervisor • (if necessary) appoint deputy supervisor
7b On-the-job consultation FREQUENCY (AND ATTENTION FOR INTEGRITY)	No or few consultations focused on integrity (less than once a month); risk: • acting at one's own discretion • insufficient (social) control • insufficient alertness to or awareness of integrity requirement	Prevent solo actions, stimulate (social) control and attention for integrity through: • regular consultations (at least once a month) • integrity as a permanent item on the agenda
7c On-the-job consultation JOB APPRAISAL INTERVIEWS	Job appraisal interviews less than once a year and/or no attention for vulnerable aspects; risk: • inadequate control, guidance, supervision and correction • reduced alertness and awareness	Stimulate control and alertness by periodic job appraisal interviews (at least once a year) in which attention is paid to integrity aspects
8 External contacts	supervisor is not aware of external contacts of employees; risk: • inadequate control • reduced opportunity to identify risky contacts • solo action	Prevent solo actions, stimulate control and prevent conflicts of interests through: • obligatory reports of discussions • keeping files of liaisons • external contacts as a permanent item on the agenda (cf. 7)
9 Accounting and supervision	Frequency of giving account of vulnerable activities is insufficient (cf. stage A); risk: • inadequate supervision • solo action • acting at one's own discretion Only routine checks by supervisor; risk: • inadequate control	Stimulate the correct and careful performance of vulnerable duties in a preventive sense and if necessary correct mistakes through: • asking employees to give account as regularly as possible • overall supervision or representative random checks of work
10 Interfaces business/ private life	Private problems affecting the job are not discussed; risk: • breach of integrity caused by insufficient recognition of tensions and conflict situations. Official decisions with consequences for private life are handled by one person; risk: • breach of integrity caused by insufficient recognition of complex of interests	Prevent breach of integrity as a result of interfaces between business and private life through: • the creation of a working climate in which private problems can be discussed • the appointment of a company social worker • obligation to report decisions with consequences for private life to the supervisor • delegating or sharing such decisionmaking

Aspects	Problems	Suggestions for possible solutions
11 Malafide outsiders	Attempted violations of integrity are not reported; risk: • undermining of the organisation	Stimulate company-wide alertness through: • obligation to report attempted violations of integrity to the supervisor
12 Malafide employees	Lack of, unknown and/or not applied guidelines on how to deal with malafide employees; risk: • inconsistent approach and correction of violations (arbitrariness) • no awareness of the consequences of corruptible behaviour	Prevent corruptible behaviour by employees through: • drawing up guidelines (and imposing sanctions) • drawing attention to these guidelines • consistent application of the guidelines • drawing attention to this application
13a Specific regulations CONFIDENTIAL INFORMATION	Lack of, unknown and/or not applied regulations; risk: • (too) low thresholds against leaking of information • insufficient alertness • (too) much pressure on personal carefulness	Prevent inspection by unauthorized persons through: • drawing up regulations for the handling of information (production, mutation, distribution, duplication, administration, storing, etc.) • wide distribution of the regulations • supervision of consistent application • imposing sanctions on non-compliance
13b Specific regulations FUNDS AND BUDGETS	Lack of, unknown and/or not applied regulations; risk: • (too) low thresholds against malversation • insufficient alertness • (too) much pressure on personal carefulness	Prevent malversation by: • drawing up regulations for handling funds and expense claims (granting, control, spending, payments) • wide distribution of the regulations • imposing sanctions on noncompliance • independent audit
13c Specific regulations PURCHASE OF GOODS AND HIRING SERVICES	Lack of, unknown and/or not applied regulations; risk: • (too) low thresholds against malversation • insufficient alertness • (too) much pressure on personal carefulness	Prevent fraud and conflict of interests by: • drawing up regulations for buying goods or hiring services (concerning quality demands, terms of delivery, quotations, negotiations with suppliers, tenders) • wide distribution of the regulations • supervision of the compliance • imposing sanctions on non-compliance
13d Specific regulations PRIVATE USE OF GOODS AND SERVICES	Lack of, unknown and/or not applied regulations; risk: • (too) low thresholds against unlawful appropriation • (too) much pressure on personal perception of integrity	Prevent unlawful use by: • drawing up regulations for the private use of goods and services • wide distribution of the regulations • supervision of the compliance • imposing sanctions on non-compliance

Aspects	Problems	Suggestions for possible solutions
14 Business gifts, additional functions/ income	Lack of, unknown and/or not applied regulations; risk: • conflict of interests • (too) much pressure on personal perception of integrity	Prevent conflict of interests by drawing up regulations, distributing them widely, supervising the compliance (and if necessary imposing sanctions on non-compliance).
15 Physical security	Inadequate provisions; risk: • (too) low thresholds against violations of integrity by third parties	Prevent integrity violations by outsiders through adequate physical security(entrance checks, duty to identify oneself, registration and escort of visitors, locking offices, closets, desks, etc.)
16 Lawfulness versus efficiency	Disproportional attention for efficiency at the expense of lawfulness; risk: • (too) much pressure on personal perception of integrity	Increase emphasis on lawfulness and decrease pressure on personal perception of integrity by focusing on measures mentioned under 4, 5, 8 and 9.
17 Loyalty	Insufficient loyalty or exaggerated loyalty with one's own department or colleagues; risk: • (too) little attention for general interest • defiant behaviour • covering up of mistakes or shortcomings	Reduce the risk by focusing on measures mentioned under 8, 10 and 14, and stimulate loyalty with the (total) organisation by drawing up a general code of conduct
18 Communication	Inadequate internal communication; risk: • gap between management and employees • no clarity about activities of colleagues • reduced social control	Reduce the risk by focusing on the measures mentioned under 4, 7, 8, 13 and 14, and stimulate internal communication (possibly also lay down agreements in a general code of conduct)
19 Selfcorrection	Inadequate self-correction; risk: • decreased ability to defend oneself against integrity violations (identification, approach and making sure it does not happen again)	Enhance the ability to defend oneself through all aforementioned aspects, with special attention for: • creating a working climate which leaves room for criticism and in which criticism is taken seriously and employees (at all levels) are held responsible for their mistakes • accounting and supervision (cf. 9) • obligation to report as mentioned under 10 and 11 • compliance with guidelines (including sanctions) as mentioned under 12 In addition, remove barriers for reporting and handling integrity violations by the appointment of a special counselor